PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G07F	A2	(11) Internationale Veröffentlichungsnummer: **WO 97/46983**
		(43) Internationales Veröffentlichungsdatum: 11. Dezember 1997 (11.12.97)

(21) Internationales Aktenzeichen: PCT/EP97/02894

(22) Internationales Anmeldedatum: 4. Juni 1997 (04.06.97)

(30) Prioritätsdaten:
196 22 533.7 5. Juni 1996 (05.06.96) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: SCHAEFER-LORINSER, Frank [DE/DE]; Potsdamer Strasse 88, D-64372 Ober-Ramstadt (DE). SCHEERHORN, Alfred [DE/DE]; Ahornallee 3, D-49716 Meppen (DE).

(81) Bestimmungsstaaten: AU, BR, CA, CN, HU, JP, KR, MX, NO, TR, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: METHOD AND DEVICE FOR LOADING INPUT DATA INTO AN ALGORITHM DURING AUTHENTICATION

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUM LADEN VON INPUTDATEN IN EINEN ALGORITHMUS BEI DER AUTHENTIKATION

(57) Abstract

The problem associated with data security during payment transactions using smart cards lies in the processes involved in loading input data into an algorithm during authentication. According to the invention, the security of the withdrawal and charging data is improved by dividing the data blocks and switching an additional feedback to the downstream counters on and off at pre-selected times (cycles). The invention can be used in all authentication processes involving smart cards.

(57) Zusammenfassung

Die Problematik der Datensicherheit beim Zahlungsverkehr mit Hilfe von Chipkarten liegt in den Vorgängen beim Laden von Inputdaten in einen Algorithmus bei der Authentikation begründet. Mit Hilfe einer Aufteilung der Datenblöcke und der Ein- und Ausschaltung einer zusätzlichen Rückkopplung nach den nachgeschalteten Zählern zu vorgewählten Zeiten (Takten) wird die Sicherheit der Ab- und Aufbuchungs-Daten verbessert. Die Anwendung der Erfindung ist bei allen Authentikationsvorgängen in Verbindung mit Chipkarten möglich.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verfahren und Vorrichtung zum Laden von Inputdaten in einen Algorithmus bei der Authentikation

Beschreibung:

Die Erfindung bezieht sich auf ein Verfahren, wie im Oberbegriff des Patentanspruch 1 näher beschrieben und auf eine Vorrichtung der im Oberbegriff des Patentanspruch 9 definierten Art. Verschiedene bekannte Verfahren dieser Art werden für Chipkarten mit Börsenfunktion in mehreren Varianten verwendet und bei den Vorrichtungen kann u. a. von Chipschaltungen entsprechend EP 0 616 429 A1 ausgegangen werden.

Verfahren der hier gemeinten Art sind z. B. aus ETSI D/EN/TE 090114, Terminal Equipment (TE) Requirements for IC cards and terminals for telecommunication use, Part 4 - Payment methods Version 4 v. 07. Febr. 1992 und aus der Europäischen Patentanmeldung 0 605 070 bekannt.

Neben Telefonkarten mit definiertem Anfangsguthaben als Zahlungsmittel für Kartentelefone sind auch "elektronische Geldbörsen" nach dem gleichen Prinzip als Zahlungsmittel für begrenzte Beträge von zunehmender Bedeutung. Für den Anwendungsfall "Bezahlen mit der Chipkarte" ist ein entsprechendes Kartenlesermodul mit einem Sicherheitsmodul SM zur Karten- und Guthabenprüfung in den Automaten gekoppelt.

Aus der EP 0 605 070 A2 ist auch ein Verfahren zum Transferieren von Buchgeldbeträgen auf und von Chipkarten bekannt, bei dem überschreibbare Speicherplätze einer Chipkarte aufgeteilt werden in wenigstens zwei Speicherplätze, von denen einer als "debitorisch", also "elektronische Geldbörse" ge-

nutzt wird, so wie die Telefonkarten, und der andere "kreditorisch" im Sinne einer Kreditkarte. Unter den für Kreditkarten üblichen gesicherten Bedingungen ist es vorgesehen, Geldbeträge zwischen den Bereichen zu transferieren, um die "elektronische Geldbörse" wieder aufzufüllen.

Zur Vermeidung sowohl der Gefahren unbefugter Zugriffe auf die Kassenautomaten und deren fest im Gerät integrierte Sicherheitsmodule, als auch der Notwendigkeit von besonders geschützten und deshalb für den Betreiber teuren Standleitungen wurde mit (P95114) ein Verfahren vorgeschlagen, bei dem vom Betreiber des Kassenautomaten vor den Kassiervorgängen ein Sicherheitsmodul mit Chipkartenfunktionen in die Kassenautomaten eingesteckt wird und bei jedem Kassiervorgang, bei dem ein Kartennutzer seine Chipkarte mit Börsenfunktion in einen Kassenautomaten eingesteckt hat, zuerst Datenbereiche der Chipkarte für eine Plausibilitätskontrolle und die Prüfung des Restguthabens ausgelesen, danach eine Authentifikation mit dem Sicherheitsmodul und eine ein-/mehrmalige Akzeptanzentscheidung durchgeführt werden und bei dem zuletzt der fällige bzw. eingegebene Geldbetrag aus der Chipkarte des Kartennutzers mit Hilfe einer Sicherheitsfunktion ab- und einem Summenzähler für Geldbeträge im Sicherheitsmodul aufgebucht werden und bei dem nach den Kassiervorgängen der Zählerstand des Sicherheitsmoduls mit Chipkartenfunktionen an eine Abrechnungszentrale übergeben wird.

Aufgabe der Erfindung ist es, die Sicherheit der Kassenautomaten für die "elektronischen Geldbörsen" gegenüber Manipulationen und Fehlfunktionen noch weiter zu erhöhen.

Diese Aufgabe löst ein Verfahren entsprechend dem Kennzeichen des Patentanspruchs 1.

Vorteilhafte Aus- bzw. Weiterbildungsmöglichkeiten dieses Verfahrens sind in den Kennzeichen der Unteransprüche 2 bis 8 aufgeführt.

Im Kennzeichen des Patentanspruchs 9 ist eine für die Anwendung des erwähnten Verfahrens geeignete Vorrichtung beschrieben.

Die Kennzeichen der Unteransprüche 10 bis 14 nennen vorteilhafte Aus- bzw. Weiterbildungsmöglichkeiten dieser Vorrichtungen für verschiedene Anwendungen .

Die Erfindung ist mit ihren Wirkungen, Vorteilen und Anwendungsmöglichkeiten in den nachfolgenden Ausführungsbeispielen näher beschrieben.

Authentikationsalgorithmen werden i. A. zur sicheren Identifizierung verwendet. In Authentikationsverfahren gehen, neben der Identität von Chipkarten und Personen sowie evtl. eines Sicherheitsmoduls SM, oft noch weitere Daten ein, deren Korrektheit zusätzlich gesichert werden soll. Ein Authentikationsverfahren kann zum Beispiel auch auf nicht geheime Kartendaten D zusammen mit einem geheimen Schlüssel K und einer Zufallszahl Z angewendet werden. Bei den Chipkarten mit Börsenfunktion wird für die Ab- und Aufbuchungen sicherheitshalber je eine getrennte Sicherheitsfunktion verwendet, die jeweils mit einer kryptografischen Prüfsumme ausgelesen wird.

Mit dem Verfahren nach der Erfindung können die Ab- und Aufbuchungen mit einem kryptografischen Token durchgeführt werden, wobei vorausgesetzt wird, daß die Authentikation und die kryptografische Prüfsumme über den Zählerstand mit einem Challenge/Response-Verfahren durchgeführt werden. Dann kann durch ein einzelnes Challenge/Response-Verfahren, bei dem nur eine Zufallszahl von dem Sicherheitsmodul SM

geliefert wird und von der Chipkarte nur eine Response berechnet wird, sowohl die Identität (Authentikation) als auch der interne Zählerstand gegenüber dem Sicherheitsmodul SM bewiesen werden.

Dies kann dadurch erreicht werden, daß die variablen Inputdaten, wie der Zählerstand und die Zufallszahl, intern jeweils zunächst mit "keyed Hashfunctions" = MAC Funktionen bearbeitet werden. Dabei wird als Schlüssel der kartenindividuelle geheime Schlüssel der Chipkarte verwendet. Die beiden aus Zählerstand und Zufallszahl gewonnenen Token können dann in -möglicherweise kryptografisch unsicherer Art - z. B. durch XOR oder ein linear rückgekoppeltes Schieberegister miteinander verknüpft werden und hiernach mit einer kryptografischen Funktion ausreichender Stärke integritätsgeschützt ausgegeben werden.

Diese Verfahrensweise ist für die Praxis dadurch interessant, daß die nur intern verwendeten keyed Hashfunctions keinen besonders hohen Ansprüchen hinsichtlich ihrer Sicherheit genügen müssen und relativ einfache Funktionen anwendbar sind, weil die Ergebnisse dieser Funktionen nicht aus der Chipkarte nach außen geführt werden. Dennoch werden damit Datenmanipulationen wirksam verhindert.

Das Ausführungsbeispiel der Erfindung geht von einem linear rückgekoppelten Schieberegister LFSR mit zusätzlicher nichtlinearer Funktion und nachgeschalteten Zählern aus:

0. Zusätzliche Rückkopplungen nach den nachgeschalteten Zählern in das linear rückgekoppelte Schieberegister LFSR werden geschaltet.

1. Es werden Inputdaten, bestehend aus den nicht geheimen Kartendaten D und dem geheimen Schlüssel K, in das linear rückgekoppelten Schieberegister LFSR eingelesen,

während sowohl die Rückkopplung des linear rückgekoppelten Schieberegisters LFSR, als auch die zusätzliche(n) Rückkopplung(en) aktiv sind.

2. Es wird eine gewisse Anzahl von Takten weitergeschaltet, ohne daß zusätzliche Inputdaten eingelesen werden.

3. Es werden Inputdaten, bestehend aus der Zufallszahl R, eingelesen, während sowohl die Rückkopplung des LFSR, als auch die zusätzliche Rückkopplung(en) aktiv sind.

4. Es werden die zusätzlichen Rückkopplungen ausgeschaltet und ggf. die Zähler geändert.

5. Es wird eine gewisse Anzahl von Takten weitergeschaltet und während dieser Takte gemäß der aktuellen Zählerstände Outputbits erzeugt.

Patentansprüche:

1. Verfahren zum Laden von Inputdaten in einen Algorithmus bei der Authentikation zwischen Chipkarten mit Börsenfunktion und einem Sicherheitsmodul, bei dem der Kartennutzer über ein gespeichertes Guthaben verfügen kann und bei dem bei jedem Kassiervorgang der erforderliche, bzw. der vom Kartennutzer eingegebene Geldbetrag aus der Chipkarte des Kartennutzers mit Hilfe einer Sicherheitsfunktion abgebucht und die Geldbeträge in einem Summenzähler für Geldbeträge des Sicherheitsmoduls aufaddiert und gespeichert werden, und bei dem für den Authentikationsalgorithmus ein linear rückgekoppeltes Schieberegister verwendet wird, dessen nichtlineare Funktionen in Verbindung mit nachgeschalteten Zählern kryptografisch verstärkt wird, und bei dem Inputdaten, wie z. B. eine Zufallszahl, ein geheimer Schlüssel und nicht geheime Kartendaten, in diesen Algorithmus eingehen, dadurch gekennzeichnet, daß die Inputdaten in mehrere Blöcke von Daten aufgeteilt werden und daß während des Ladens der Blöcke in das linear rückgekoppelte Schieberegister eine zusätzliche weitere Rückkopplung nach den nachgeschalteten Zähler in das Schieberegister eingeführt und nach einer vorgegebenen Anzahl von Taktschritten abgeschaltet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Kartendaten D mit einem geheimen Schlüssel K als ein erster Block und eine Zufallszahl R als ein weiterer Block eingeführt werden.

3. Verfahren nach Anspruch 1 und 2, dadurch gekennzeichnet, daß während der Ladephase der Inputdaten andere Zählerstände eingesetzt werden, als bei der darauffolgenden Phase nach Einladen der Inputdaten zur Berechnung des Authentikationstokens.

4. Verfahren nach Anspruch 1 und 2, dadurch gekennzeichnet, daß der erste nachgeschaltete Zähler auf 1 zählt.

5. Verfahren nach Ansprüch 1 und 2, dadurch gekennzeichnet, daß die Zähler und die Anzahl der auszuführenden Takte genau so gewählt werden, daß das Authentikationstoken nach einer durch andere Systembedingungen fest vorgegebenen Anzahl von Takten errechnet wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Ausgabe von Bits nach Einladen aller Inputdaten beginnt.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß zwischen dem Einladen der Blöcke aus Anspruch 1 unter Beibehaltung der zusätzlichen Rückkopplung die gesamte Schaltung einige Schritte weiter getaktet wird, ohne daß Inputdaten geladen werden und bevor Bits ausgegeben werden.

8. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß zwischen dem Einladen der Blöcke aus Anspruch 1 nach Abschalten der zusätzlichen Rückkopplung die gesamte Schaltung eine bestimmte Anzahl von Schritten weiter getaktet wird, ohne daß Inputdaten geladen werden und bevor Bits ausgegeben werden.

9. Vorrichtung zum Laden von Inputdaten in einen Algorithmus bei der Authentikation unter Verwendung einer

kryptografischen MAC Funktion, bestehend aus einem linear rückgekoppelten Schieberegister mit einer nichtlinearen "Feed Forward" Funktion, die aus dem Schieberegister abgreift und über einen Zähler den Output des Schieberegisters beeinflußt, dem ein weiterer Zähler nachgeschaltet ist, dadurch gekennzeichnet, daß die aus dem linear rückgekoppelten Schieberegister aufgebaute Schaltung mit nachgeschalteten Zählern zur Verwendung für den Authentikationsalgorithmus durch eine zusätzliche abschaltbare nichtlineare Rückkopplung kryptografisch verstärkt ist.

10. Vorrichtung nach Anspruch 9 , dadurch gekennzeichnet, daß die zusätzliche Rückkopplung nach dem ersten nachgeschalteten Zähler vor dem Latch abgegriffen ist.

11. Vorrichtung nach Anspruch 9 , dadurch gekennzeichnet, daß die zusätzliche Rückkopplung aus dem Latch nach dem ersten nachgeschalteten Zähler abgegriffen ist.

12. Vorrichtung nach Anspruch 9 , dadurch gekennzeichnet, daß die zusätzliche Rückkopplung nach dem zweiten nachgeschalteten Zähler abgegriffen ist.

13. Vorrichtung nach Anspruch 9 , dadurch gekennzeichnet, daß die zusätzliche Rückkopplung als eine XOR-Summe der Abgriffe nach dem ersten nachgeschalteten Zähler vor dem Latch, aus dem Latch nach dem ersten nachgeschalteten Zähler und nach dem zweiten nachgeschalteten Zähler ausgebildet ist.

14. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die Zähler aufgeteilt bzw. verkleinert sind.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
P95140WOEK16			
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*	
PCT/EP 97/02894	04/06/1997	05/06/1996	
Anmelder			
DEUTSCHE TELEKOM AG et al.			

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

2. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

3. [ ] In der internationalen Anmeldung ist **ein Protokoll einer Nucleotid- und/oder Aminosäuresequenz** offenbart; die internationale Recherche wurde auf der Grundlage des Sequenzprotokolls durchgeführt,
   - [ ] das zusammen mit der internationalen Anmeldung eingereicht wurde.
   - [ ] das vom Anmelder getrennt von der internationalen Anmeldung vorgelegt wurde,
     - [ ] dem jedoch keine Erklärung beigefügt war, daß der Inhalt des Protokolls nicht über den Offenbarungsgehalt der internationalen Anmeldung in der eingereichten Fassung hinausgeht.
   - [ ] das von der Internationalen Recherchenbehörde in die ordnungsgemäße Form übertragen wurde.

4. Hinsichtlich der **Bezeichnung der Erfindung**
   - [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.
   - [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt.

5. Hinsichtlich der **Zusammenfassung**
   - [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.
   - [ ] wurde der Wortlaut nach Regel 38.2b) in der Feld III angegebenen Fassung von dieser Behörde festgesetzt. Der Anmelder kann der Internationalen Recherchenbehörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen:
   Abb. Nr. _____
   - [ ] wie vom Anmelder vorgeschlagen
   - [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
   - [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

   [X] keine der Abb.

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
G07F 7/10, H04L 9/26

A3

(11) Internationale Veröffentlichungsnummer: WO 97/46983

(43) Internationales Veröffentlichungsdatum: 11. Dezember 1997 (11.12.97)

(21) Internationales Aktenzeichen: PCT/EP97/02894

(22) Internationales Anmeldedatum: 4. Juni 1997 (04.06.97)

(30) Prioritätsdaten:
196 22 533.7 5. Juni 1996 (05.06.96) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: SCHAEFER-LORINSER, Frank [DE/DE]; Potsdamer Strasse 88, D-64372 Ober-Ramstadt (DE). SCHEERHORN, Alfred [DE/DE]; Ahornallee 3, D-49716 Meppen (DE).

(81) Bestimmungsstaaten: AU, BR, CA, CN, HU, JP, KR, MX, NO, TR, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 26. Februar 1998 (26.02.98)

(54) Title: METHOD AND DEVICE FOR LOADING INPUT DATA INTO AN ALGORITHM DURING AUTHENTICATION

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUM LADEN VON INPUTDATEN IN EINEN ALGORITHMUS BEI DER AUTHENTIKATION

(57) Abstract

The problem associated with data security during payment transactions using smart cards lies in the processes involved in loading input data into an algorithm during authentication. According to the invention, the security of the withdrawal and charging data is improved by dividing the data blocks and switching an additional feedback to the downstream counters on and off at pre-selected times (cycles). The invention can be used in all authentication processes involving smart cards.

(57) Zusammenfassung

Die Problematik der Datensicherheit beim Zahlungsverkehr mit Hilfe von Chipkarten liegt in den Vorgängen beim Laden von Inputdaten in einen Algorithmus bei der Authentikation begründet. Mit Hilfe einer Aufteilung der Datenblöcke und der Ein- und Ausschaltung einer zusätzlichen Rückkopplung nach den nachgeschalteten Zählern zu vorgewählten Zeiten (Takten) wird die Sicherheit der Ab- und Aufbuchungs-Daten verbessert. Die Anwendung der Erfindung ist bei allen Authentikationsvorgängen in Verbindung mit Chipkarten möglich.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

INTERNATIONAL SEARCH REPORT

Inter ɔnal Application No
PCT/EP 97/02894

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 H04L9/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 44 19 805 A (GIESECKE & DEVRIENDT) 7 December 1995 see abstract; claims; figures see column 5, line 63 - column 6, line 31	1,2,5,6, 9,13
A	EP 0 409 701 A (ETAT FRANCAIS) 23 January 1991	
A	FR 2 471 003 A (ELECTRONIQUE MARCEL DASSAULT) 12 June 1981	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 November 1997	05. 12. 97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inter[illegible]lication No
PCT/EP 97/02894

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4419805 A	07-12-95	AU 2787295 A	04-01-96
		CA 2168891 A	14-12-95
		CN 1131991 A	25-09-96
		WO 9534054 A	14-12-95
		EP 0712520 A	22-05-96
		JP 9501529 T	10-02-97
EP 0409701 A	23-01-91	FR 2650097 A	25-01-91
		DE 69012692 D	27-10-94
		DE 69012692 T	19-01-95
		JP 3141487 A	17-06-91
		US 5128997 A	07-07-92
FR 2471003 A	12-06-81	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 97/02894

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G07F7/10 H04L9/26

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G07F H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 44 19 805 A (GIESECKE & DEVRIENDT) 7.Dezember 1995 siehe Zusammenfassung; Ansprüche; Abbildungen siehe Spalte 5, Zeile 63 - Spalte 6, Zeile 31	1,2,5,6, 9,13
A	EP 0 409 701 A (ETAT FRANCAIS) 23.Januar 1991	
A	FR 2 471 003 A (ELECTRONIQUE MARCEL DASSAULT) 12.Juni 1981	

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
11.November 1997	05. 12. 97

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 97/02894

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 4419805 A	07-12-95	AU 2787295 A	04-01-96
		CA 2168891 A	14-12-95
		CN 1131991 A	25-09-96
		WO 9534054 A	14-12-95
		EP 0712520 A	22-05-96
		JP 9501529 T	10-02-97
EP 0409701 A	23-01-91	FR 2650097 A	25-01-91
		DE 69012692 D	27-10-94
		DE 69012692 T	19-01-95
		JP 3141487 A	17-06-91
		US 5128997 A	07-07-92
FR 2471003 A	12-06-81	KEINE	